

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-290224

(43)Date of publication of application : 27.10.1998

(51)Int.Cl.

H04L 9/32
G09C 1/00

(21)Application number : 10-011859

(71)Applicant : FUJITSU LTD

(22)Date of filing : 23.01.1998

(72)Inventor : KOMURA MASAHIRO
ONO KOSHIO
KURODA YASUTSUGU
TORII SATORU

(30)Priority

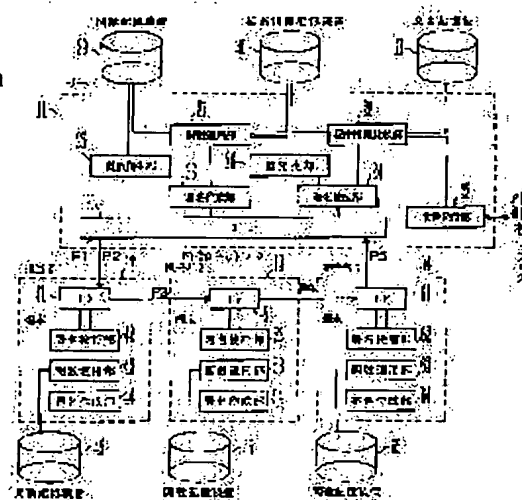
Priority number : 09 30868 Priority date : 14.02.1997 Priority country : JP

(54) AUTHENTICATION SYSTEM FOR AUTHENTICATING ELECTRONIC INFORMATION AND ITS METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent illegal electronic transaction by authenticating whether or not a person handling a document in an enterprise has a right.

SOLUTION: A value generating section 26 of a server 11 generates a proper value for authentication and sends it to a terminal 12 of a person in charge 1. The terminal 12 applies a given function to the value to generate a function value and it is added to a document and circulates it to persons in charge 2, 3. Terminals 13, 14 similarly applies a function to the value and the three application results of the 3 functions are sent to the server 11 with the document. A secret information comparison section 28 compares the received function value with a function value in a secret information storage device 30 and when they are equal, a document transmission section 22 adds an electronic signature of a representative to the document and transmits the document to outside of the enterprise.



LEGAL STATUS

[Date of request for examination] 09.03.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3898322

[Date of registration] 05.01.2007

[Number of appeal against examiner's decision of rejection]

CZ

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-290224

(43) 公開日 平成10年(1998)10月27日

(51) Int.Cl.⁹

識別記号

F I

H 0 4 L 9/32

H 0 4 L 9/00

6 7 5 D

G 0 9 C 1/00

6 4 0

G 0 9 C 1/00

6 4 0 D

6 4 0 B

6 4 0 E

H 0 4 L 9/00

6 7 3 E

審査請求 未請求 請求項の数22 O L (全 16 頁) 最終頁に続く

(21) 出願番号 特願平10-11859

(22) 出願日 平成10年(1998)1月23日

(31) 優先権主張番号 特願平9-30868

(32) 優先日 平9(1997)2月14日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(72) 発明者 小村 昌弘

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(72) 発明者 小野 越夫

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(74) 代理人 弁理士 大曾 義之 (外1名)

最終頁に続く

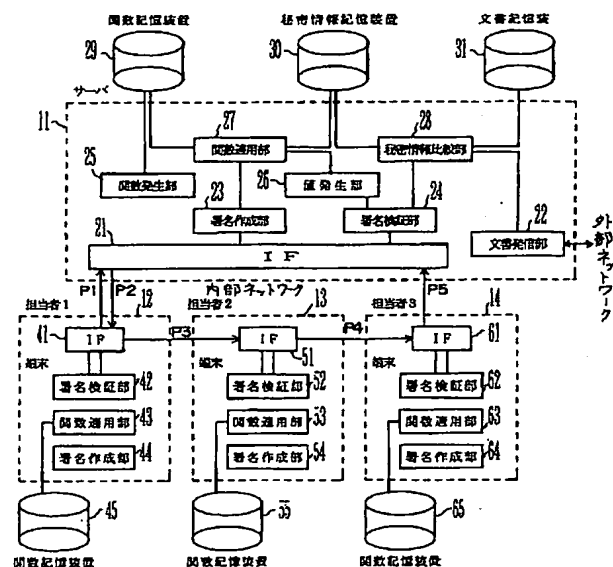
(54) 【発明の名称】 電子情報の認証を行う認証システムおよび方法

(57) 【要約】

【課題】 企業内で文書を扱った人物が権限を持っていたかどうかを検証し、電子的な不正取引を防止することが課題である。

【解決手段】 サーバ11の値発生部26は、検証用の適当な値を発生させ、担当者1の端末12に送る。端末12は、与えられた関数をその値に適用して関数値を生成し、それを文書に付加して担当者2、3に回送する。端末13、14も同様にして関数を適用し、最終的に3つの関数の適用結果が文書とともにサーバ11に送られる。秘密情報比較部28は、受け取った関数値を秘密情報記憶装置30内の関数値と比較し、それらが同じであれば、文書発信部22が、文書に代表の電子署名を付加して社外に発信する。

認証システムの構成図



【特許請求の範囲】

【請求項 1】 回送される電子情報に対応する秘密情報を格納する秘密情報格納手段と、

前記秘密情報と前記電子情報に付加された情報とに基づいて、該電子情報が正しく回送されたかどうかを確認する確認手段とを備えることを特徴とする認証装置。

【請求項 2】 正しく回送されたことが確認された確認済み電子情報に対して、代表者の電子署名を自動的に付加し、該確認済み電子情報を発信する発信手段をさらに備えることを特徴とする請求項 1 記載の認証装置。

【請求項 3】 前記秘密情報格納手段は、前記電子情報を扱う一人以上の担当者のそれぞれに割り当てられた関数をあらかじめ検証用データに適用した結果を、前記秘密情報として格納し、前記確認手段は、前記電子情報に前記検証用データが付加されて前記一人以上の担当者に回送される間に該検証用データに対して前記関数が適用された結果を、前記秘密情報と比較することで、該電子情報が正しく回送されたかどうかを確認することを特徴とする請求項 1 記載の認証装置。

【請求項 4】 前記検証用データとして、ランダムな値を発生させる値生成手段と、該ランダムな値を前記一人以上の担当者のうちの一人に送る通信手段とをさらに備えることを特徴とする請求項 3 記載の認証装置。

【請求項 5】 前記検証用データとして、前記電子情報のハッシュ値を生成する値生成手段と、該ハッシュ値を前記一人以上の担当者のうちの一人に送る通信手段とをさらに備えることを特徴とする請求項 3 記載の認証装置。

【請求項 6】 各担当者毎に前記関数を生成する関数生成手段と、該関数を各担当者毎に対応させて格納する関数格納手段とをさらに備えることを特徴とする請求項 3 記載の認証装置。

【請求項 7】 前記関数生成手段は、ハッシュ関数、秘密鍵暗号アルゴリズムの暗号化関数、および公開鍵暗号アルゴリズムの復号化関数のうちの 1 つを生成することを特徴とする請求項 6 記載の認証装置。

【請求項 8】 回送される電子情報を受け取り、次の送付先に送る通信手段と、

前記電子情報に付加された情報を、特定の担当者に割り当てられたアルゴリズムに従って変換する変換手段とを備えることを特徴とする請求項 7 記載の装置。

【請求項 9】 前記アルゴリズムとして、前記特定の担当者に割り当てられた関数を格納する関数格納手段をさらに備え、前記変換手段は、前記電子情報に付加された情報に該関数を適用し、前記通信手段は、該関数の適用結果を前記電子情報に付加して前記次の送付先に送ることを特徴とする請求項 8 記載の端末装置。

【請求項 10】 前記関数格納手段は、前記関数を他の担当者に分らないように格納することを特徴とする請求項 9 記載の端末装置。

【請求項 11】 前記関数格納手段は、前記関数を前記特定の担当者に分らないように格納することを特徴とする請求項 10 記載の端末装置。

【請求項 12】 前記関数格納手段は、取り外し可能であることを特徴とする請求項 9 記載の端末装置。

【請求項 13】 前記電子情報に付加された電子署名を検証する署名検証手段と、前記電子情報に前記特定の担当者の電子署名を付加する署名作成手段とをさらに備えることを特徴とする請求項 8 記載の端末装置。

【請求項 14】 企業間取引に関する情報を、企業内の一人以上の担当者に回送するシステムのための認証システムであって、

前記一人以上の担当者に回送された電子情報を受け取る通信手段と、

前記電子情報に付加された情報に基づいて、該電子情報が正しく回送されたかどうかを確認する確認手段とを備えることを特徴とする認証システム。

【請求項 15】 正しく回送されたことが確認された確認済み電子情報に対して、前記企業の代表者の電子署名を自動的に付加し、該確認済み電子情報を相手企業に発信する発信手段をさらに備えることを特徴とする請求項 14 記載の認証システム。

【請求項 16】 前記一人以上の担当者のそれぞれに関数を割り当てる関数付与手段をさらに備え、前記確認手段は、前記関数をあらかじめ検証用データに適用した結果を、前記電子情報に前記検証用データが付加されて回送される間に該検証用データに対して前記関数が適用された結果と比較することで、該電子情報が正しく回送されたかどうかを確認することを特徴とする請求項 14 記載の認証システム。

【請求項 17】 コンピュータのためのプログラムを記録した記録媒体であって、

回送される電子情報に対応する秘密情報を格納する機能と、

前記秘密情報と前記電子情報に付加された情報とに基づいて、該電子情報が正しく回送されたかどうかを確認する機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 18】 コンピュータのためのプログラムを記録した記録媒体であって、

回送される電子情報を受け取り、次の送付先に送る機能と、

前記電子情報に付加された情報を、特定の担当者に割り当てられたアルゴリズムに従って変換する機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 19】 企業間取引に関する情報を企業内の一人以上の担当者に回送した結果を認証するコンピュータのためのプログラムを記録した記録媒体であって、前記一人以上の担当者に回送された回送情報を受け取る

機能と、

前記回送情報に付加された情報に基づいて、該回送情報が正しく回送されたかどうかを確認する機能とを前記コンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項20】 回送情報に対応する秘密情報を生成し、

前記秘密情報と前記回送情報に付加された情報とに基づいて、該回送情報が正しく回送されたかどうかを確認することを特徴とする認証方法。

【請求項21】 回送情報を受け取り、

前記回送情報に付加された情報を、特定の担当者に割り当てられたアルゴリズムに従って変換し、
変換された情報を前記回送情報に付加して次の送付先に送ることを特徴とする回送方法。

【請求項22】 企業間取引に関する情報を企業内の一人以上の担当者に回送した結果を認証する認証方法であって、

前記一人以上の担当者に回送された回送情報を受け取り、

前記回送情報に付加された情報に基づいて、該回送情報が正しく回送されたかどうかを確認することを特徴とする認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、企業間で電子取引を行う場合などに、文書が正当な作成者および承認者を経由したかどうかを検証し、決められたルートを正しく回送された文書に代表の電子署名を付与する認証システムおよびその方法に関する。

【0002】

【従来の技術】近年、企業の従業者による不正取引が企業にとって問題となっている。最近の不正取引の特徴として、金額の巨大化、不正の長期化が挙げられ、不正取引を防止することは企業にとって重大な課題となっている。また、最近のインターネットの流行により、企業間で電子取引を開始しようとする動きがあるが、この電子取引においても、不正取引を未然に防止することが求められている。

【0003】電子取引については、最近の暗号技術を利用した認証技術の発達により、コンピュータ・ネットワーク上で個人を電子的に認証することが可能となった。例えば、ユーザAがユーザBに文書を送る場合、ユーザAは自分の電子署名を文書に付けて送る。すると、その文書を受け取ったユーザBは、電子署名がユーザAのものであることを検証することにより、受け取った文書が間違いなくユーザAが作成した文書であることを確認することができる。

【0004】

【発明が解決しようとする課題】しかしながら、ネット

ワークを利用した電子取引には次のような問題がある。

上述のような認証技術を企業内でやりとりされる文書に利用することで、文書作成や文書承認者などの文書を扱った担当者を特定することができる。しかし、認証技術はあくまで個人を特定するもので、文書を作成した人物が誰であるかは特定できるが、本当にその人物がその文書を作成する権限を持っていたかどうかは特定できない。同様に、文書を承認した人物が誰であるかは特定できるが、本当にその人物がその文書を承認する権限を持っていたかどうかは特定できない。

【0005】企業内でやり取りされる文書の場合、誰が文書を扱ったのかが分かるだけでは不十分であり、文書を扱った者がその文書を扱う権限を持っていたかどうか重要となる。

【0006】また、企業間で電子取引を行う場合、例えばA企業からB企業に文書を送信するとすると、A企業では送信する文書が間違いなくA企業で作成されたものであることを示すために、送信文書にA企業の代表の電子署名をつける。B企業は、受信文書につけられた電子署名を検証することで、文書が間違いなくA企業で作成されたものであることを確認できる。

【0007】ここで、A企業において、代表の電子署名を付ける手段を、文書を作成もしくは検査する担当者に与えると、その担当者が本来の業務に関係のない文書にまで代表の電子署名を付けて、不正取引を行うことが可能となり、非常に危険である。よって、企業間で電子取引を安全に行うためには、文書を送信する企業内で、文書を送信する直前に代表の電子署名を文書に付けるようなシステムが必要となる。

【0008】本発明の課題は、文書を扱った人物が文書を扱う権限を持っていたかどうかをシステムチックに検証し、検証された文書に対して自動的に代表の電子署名を付けることで、不正取引を防止する認証システムおよびその方法を提供することである。

【0009】

【課題を解決するための手段】図1は、本発明の認証システムの原理図である。図1の認証システムは、通信ネットワーク7に接続された認証装置1と各担当者の端末装置4から成り、認証装置1は秘密情報格納手段2と確認手段3を備え、端末装置4は通信手段5と変換手段6を備える。

【0010】秘密情報格納手段2は、回送される電子情報に対応する秘密情報を格納し、確認手段3は、上記秘密情報と上記電子情報に付加された情報とに基づいて、その電子情報が正しく回送されたかどうかを確認する。

【0011】ネットワーク7上では、文書データ、画像データなどの任意の電子情報が関係する担当者間で回送され、秘密情報格納手段2は、各電子情報に対応する秘密情報を、あらかじめそれらの担当者に知られないようにして格納している。各担当者の端末装置4を回送さ

れた電子情報が到着すると、確認手段3は、電子情報に付加された情報を取り出し、それと秘密情報とに基づいて回送ルートを確認する。

【0012】秘密情報としては、例えば、電子情報を扱う一人以上の担当者のそれぞれに割り当てられた関数を、回送順に検証用データに適用した結果が用いられる。そして、電子情報に検証用データが付加されて各担当者に回送される間に、その検証用データに対して、端末装置4により関数が適用された結果を、秘密情報と比較することで、電子情報が正しく回送されたかどうかを確認できる。

【0013】もし、両方の結果が一致しなければ、電子情報が、それを扱う権限のない担当者に回送されたか、あるいは、正規の回送ルートと異なる順序で回送された可能性があるとみなされる。このような場合には、その電子情報の発信処理を中止することができる。

【0014】そして、秘密情報と電子情報に付加された情報とが一致した場合にのみ、その電子情報に代表の電子署名を付けて社外に発信することで、従業員による不正取引を防止することができる。

【0015】また、端末装置4の通信手段5は、回送される電子情報を受け取り、次の送付先に送る。このとき、変換手段6は、受け取った電子情報に付加された情報を、特定の担当者に割り当てられたアルゴリズムに従って変換する。

【0016】特定の担当者とは、例えば、各端末装置4に割り当てられた担当者を指し、変換手段6は、その担当者にあらかじめ与えられた特定のデータ変換アルゴリズムに従って、電子情報に付加された情報を変換する。このデータ変換アルゴリズムとしては、例えば、上記関数が用いられる。

【0017】変換された情報は、通信手段5により電子情報に付加されて次の端末装置4に送られ、その端末装置4において、別のデータ変換アルゴリズムによる変換が施される。このようにして、電子情報が各担当者に回送される間に、付加情報が次々と変換されて、最終的には、回送されたルート特有の情報に変換される。認証装置1は、この情報を調べることで、電子情報が正しく回送されたかどうかを確認することができる。

【0018】そして、電子情報に付加された情報が正しい回送ルートに対応している場合にのみ、その電子情報に代表の電子署名を付けて社外に発信することで、従業員による不正取引を防止することができる。

【0019】例えば、図1の認証装置は、後述する図2におけるサーバ11に対応し、秘密情報格納手段2は秘密情報記憶装置30に対応し、確認手段3は秘密情報比較部28に対応する。また、例えば、通信手段5はインタフェース41、51、61に対応し、変換手段6は関数適用部43、53、63に対応する。

【0020】

【発明の実施の形態】以下、図面を参照しながら、本発明の実施の形態を詳細に説明する。本発明の認証システムにおいては、企業間で電子取引を安全に行うために、文書を送信する側の企業において、文書が、正当な担当者である作成者および承認者を経た場合にのみ、その文書に代表の電子署名を付けるようにする。

【0021】このため、サーバは、あらかじめ各担当者の端末に特定の関数を配っておき、文書とともに検証用の適当なデータを回送する。各端末は、与えられた関数を回送されるデータに順次適用し、関数値として次の端末に送る。そして、サーバは、最後の端末から送られた関数値を、最初のデータに各担当者の関数を回送順に適用した結果と比較して、回送ルートを検証する。

【0022】それらが一致すれば、文書が決められたルートで正しく回送されたものと判定し、自動的に、文書に代表の電子署名を付けて社外に発信する。このように、サーバのみが知っている関数と検証用データを用いることで、文書が正しい担当者を経由したかどうかチェックされ、各担当者の権限が検証される。また、サーバが代表の電子署名を付与するので、担当者による電子署名の不正使用が防止される。

【0023】電子署名とは、データの送信者が本人しか知らない秘密鍵を用いて、なんらかの方法でデータを暗号化して作成した情報である。データの受信者が、送信者の身元が確かであることを確認するためには、例えば、認証局から発行される証明書の中の公開鍵を用いて電子署名を復号化し、その内容を検証すればよい。電子署名の生成に用いられる秘密鍵と証明書に記載される公開鍵とは対になっており、秘密鍵により暗号化されたデータは公開鍵により復号化することができる。

【0024】図2は、本発明の認証システムの構成図である。図2の認証システムは、サーバ11と担当者の端末12、13、14を含み、社外の通信ネットワークである外部ネットワークに接続されている。

【0025】サーバ11は、インタフェース(IF)21、文書発信部22、署名作成部23、署名検証部24、関数発生部25、値発生部26、関数適用部27、および秘密情報比較部28を含む。サーバ11には、関数記憶装置29、秘密情報記憶装置30、および文書記憶装置31が接続されている。

【0026】また、担当者1の端末12は、インタフェース41、署名検証部42、関数適用部43、および署名作成部44を含み、担当者2の端末13は、インタフェース51、署名検証部52、関数適用部53、および署名作成部54を含み、担当者3の端末14は、インタフェース61、署名検証部62、関数適用部63、および署名作成部64を含む。

【0027】これらの端末12、13、14には、それぞれ、関数記憶装置45、55、65が接続されている。また、サーバ11と端末12、13、14は、社内

の通信ネットワークである内部ネットワークにより、互いに結合されている。なお、担当者の端末は、一般に任意の数だけ設けることができ、4台以上の場合も同様の構成を持つ。

【0028】このような認証システムにおいて、ある文書が担当者1から担当者3まで回送される場合を例に取り、その回送および発信を認証する動作を説明する。まず、文書を回送する前に、サーバ11の関数発生部25は、担当者1、担当者2、担当者3用にそれぞれ個別の関数を発生させる。サーバ11は、作成した関数を、他の担当者には知られないように各担当者に配送する。担当者1、担当者2、担当者3は、配送された関数を、それぞれ関数記憶装置45、55、65に格納する。

【0029】また、サーバ11は、各関数を関数記憶装置29に格納する。その際、図3に示すように、文書の回送ルートに従って、文書種別、発信者、受信者、および関数からなる表を作成し、発信者から文書作成通知が来た時の回送ルート検索に用いる。ここでは、担当者1、担当者2、担当者3に対して、それぞれ、関数1、関数2、関数3が割り当てられており、文書種別“文1”は、担当者1、担当者2、担当者3、サーバの順の回送ルートに対応している。

【0030】図4は、実際に文書を発信するまでの過程で、サーバ11や各端末間でやり取りされる通信データの表を示している。まず、担当者1が文書を発信する場合、手順P1において、端末12は、インタフェース41からサーバ11のインタフェース21に対して、作成した文書を送る。

【0031】サーバ11の値発生部26は、送られた文書に対するIDと、サーバ11にしか分からない適当な値を一つ生成する。取り扱う文書が種類しかない場合は、IDは必ずしも生成する必要はなく、以下の処理において省略することができる。また、値はランダムに発生させてもよく、文書またはIDの一部を値として用いてもよい。

【0032】次に、サーバ11は、文書種別と発信者の情報をもとに、関数記憶装置29から文書の回送ルートを検索し、関数適用部27において、回送ルートに含まれる担当者の各関数を、順次、値発生部26が生成した値に適用する。関数を適用された値は、秘密情報として、図5に示すように、値発生部26が生成したIDと共に秘密情報記憶装置30に格納される。

【0033】手順P2において、サーバ11は、値発生部26が生成したIDと値を、インタフェース21から端末12のインタフェース41に送る。インタフェース41を介して値を受け取った関数適用部43は、関数記憶装置45に格納された関数1を受け取った値に適用する。そして、署名作成部44は、文書、ID、および関数適用値である“関数1(値)”に、電子署名1を付ける。

【0034】このように、担当者の電子署名は、文書、ID、および関数適用値を含むデータの全体に付けるのが望ましいが、もちろん、その一部分に付けることも可能である。

【0035】手順P3において、端末12は、文書、ID、関数適用値、および電子署名1を、インタフェース41から端末13のインタフェース51に送る。インタフェース51を介してこれらの情報を受け取った署名検証部52は、担当者1が付けた電子署名1を検証する。

【0036】検証結果に誤りがなければ、関数適用部53が、関数記憶装置55に格納された関数2を、受け取った関数適用値に適用する。そして、署名作成部54は、文書、ID、および関数適用値“関数2(関数1(値))”に、電子署名2を付ける。

【0037】手順P4において、端末13は、文書、ID、関数適用値、電子署名1、および電子署名2を、インタフェース51から端末14のインタフェース61に送る。インタフェース61を介してこれらの情報を受け取った署名検証部62は、担当者2が付けた電子署名2を検証する。

【0038】検証結果に誤りがなければ、関数適用部63が、関数記憶装置65に格納された関数3を、受け取った関数適用値に適用する。そして、署名作成部64は、文書、ID、および関数適用値“関数3(関数2(関数1(値)))”に、電子署名3を付ける。

【0039】手順P5において、端末14は、文書、ID、関数適用値、電子署名1、電子署名2、および電子署名3を、インタフェース61からサーバ11のインタフェース21に送る。インタフェース21を介してこれらの情報を受け取った署名検証部24は、担当者3が付けた電子署名3を検証する。

【0040】検証結果に誤りがなければ、秘密情報比較部28は、担当者3から送られた関数適用値と、秘密情報格納装置30に格納された秘密情報とを比較する。その結果、両者の値が同一であれば、サーバ11は、文書が適切なルートで回送されたものとみなし、文書、電子署名1、電子署名2、および電子署名3を、文書記憶装置31に格納する。そして、文書発信部22が、文書に代表の電子署名を付けて社外に発信する。

【0041】このシステムでは、サーバ11が発生させた関数1、関数2、関数3は、担当者自身にも分からないようにして、それぞれ担当者1、担当者2、担当者3に渡され、関数記憶装置45、55、65に格納される。

【0042】関数の配送方法としては、ICカードなどの可搬記憶媒体を関数記憶装置として用い、これをオフラインで渡す方法、サーバ11と各端末をセキュリティの確保された専用回線で結んで、ハードウェアによりオンラインで配送する方法などがある。前者の場合は、関数記憶装置を簡単に取り外しできるというメリットがあ

る。

【0043】また、サーバ11が、発生させた値、例えばランダムな値を回送する文書に付加し、各担当者がこのランダムな値にあらかじめサーバ11から与えられた関数を適用することで、ランダムな値は各担当者にしか生成できない特定の値に変換される。

【0044】各担当者はそれぞれ同様の処理を行い、文書と関数により変換された値がサーバ11に返される。サーバ11は、各担当者に与えた関数を関数記憶装置29に格納しておき、上記のランダムな値に各関数を順に適用した結果と、各担当者が各関数をランダムな値に順に適用した結果が同じかどうかを調べることで、文書が担当者1、担当者2、担当者3の順に回送されたかどうかを確認することができる。

【0045】また、サーバ11が発生させた関数を、担当者自身にも分からないように関数記憶装置45、55、65に格納しておけば、担当者が異動になった場合にも、同じ関数が自動的に新しい担当者に与えられる。このように、関数を担当者の役職に対して一意的に付与することで、異動に簡単に対応することができる。

【0046】さらに、担当者が一時的に不在になった場合は、関数を関数記憶装置ごと代理の担当者に渡すことで、簡単に対応することができる。特に、関数記憶装置として、簡単に取り外し可能なICカードなどを用いた場合は、それを代理の担当者に渡すだけでよい。

【0047】また、関数を他の担当者に分からないようにしておくことで、他の担当者がその関数を与えられた担当者になりすますことを防止できる。この場合、各担当者は、受け取った値に他人の関数を適用することができず、したがって、文書が正しく回送されたかのように見せかけることはできない。

【0048】このように、関数は役職に対して付与されるが、電子署名は担当者個人に対して一意的に付与されており、異動に応じて変更される。文書に担当者の電子署名を付けて回送することで、問題が発生した場合に、その文書を扱った担当者を容易に特定することができる。

【0049】ところで、手順P1において、値発生部26は、受け取った文書のハッシュ値を生成して、これを検証用の値として用いることもできる。これにより、作成者である担当者1による文書のすりかえができなくなり、システムの信頼性が向上する。

【0050】また、手順P2において、サーバ11の署名作成部23は、IDと値にサーバの電子署名0を付けて端末12に送ることもできる。この場合、図4の各手順における通信データは図6に示すようになり、端末12の署名検証部42は、サーバの電子署名0を検証する。そして、検証結果に誤りがなければ、関数適用部43が関数1を受け取った値に適用する。

【0051】図7は、サーバ11や端末12、13、1

4に対応する情報処理装置（コンピュータ）の構成図である。図7の情報処理装置は、CPU（中央処理装置）71、メモリ72、入力装置73、出力装置74、外部記憶装置75、媒体駆動装置76、ネットワーク接続装置77を備え、それらの各装置はバス78により互いに結合されている。

【0052】CPU71は、メモリ72に格納されたプログラムを実行して、サーバ11や端末12、13、14の各処理を実現する。メモリ72には、各処理に用いられるプログラムとデータが格納されている。このメモリ72は、例えばROM（read only memory）、RAM（random access memory）等を含む。

【0053】入力装置73は、例えばキーボード、ポインティングデバイス等に相当し、ユーザからの要求や指示の入力に用いられる。また、出力装置74は、表示装置やプリンタ等に相当し、ユーザへの問い合わせや処理結果等の出力に用いられる。

【0054】外部記憶装置75は、例えば、磁気ディスク装置、光ディスク装置、光磁気ディスク装置等である。この外部記憶装置75に、上述のプログラムとデータを保存しておき、必要に応じて、それらをメモリ72にロードして使用することができる。また、外部記憶装置75は、関数記憶装置29、45、55、65、秘密情報記憶装置30、および文書記憶装置31としても使用され得る。

【0055】媒体駆動装置76は、可搬記録媒体79を駆動し、その記憶内容にアクセスする。可搬記録媒体79としては、メモリカード（ICカード）、フロッピーディスク、CD-ROM（compact disk read only memory）、光ディスク、光磁気ディスク等、任意のコンピュータ読み取り可能な記録媒体を使用することができる。この可搬記録媒体79に、上述のプログラムとデータを格納しておき、必要に応じて、それらをメモリ72にロードして使用することができる。さらに、可搬記録媒体79は、関数記憶装置45、55、65としても使用することができる。

【0056】ネットワーク接続装置77は、LAN（local area network）等の任意の通信ネットワークに接続され、通信に伴うデータ変換等を行う。情報処理装置は、ネットワーク接続装置77を介して、他の情報処理装置80（サーバ11、端末12、13、14等）と通信する。これにより、必要に応じて、プログラムとデータを情報処理装置80からネットワークを介して受け取り、それらをメモリ72にロードして使用することができる。

【0057】次に、図8から図10までを参照しながら、図2の認証システムによる処理の例について説明する。図8は、関数としてハッシュ関数、または秘密鍵暗号システムにおける暗号化関数を用いた認証システムを示している。ハッシュ関数とは、与えられたデータに適

当な操作を施すことで、元に戻すことのできないデータを生成する一方方向性関数であり、秘密鍵暗号システムとは、DES (Data Encryption Standard) 暗号のような秘密鍵暗号アルゴリズムを用いたシステムである。

【0058】秘密鍵暗号システムにおいては、暗号化と復号化の両方に秘密鍵を用いており、その鍵情報を知らない、暗号化も復号化も行うことができない。ここでは、各担当者毎に異なる秘密鍵を用いた暗号化関数を与えられ、それらの鍵情報を担当者は知らないものとする。暗号化のアルゴリズムは、担当者毎に異なっても同じでもよい。図8において、担当者1が文書を作成する場合の処理は、次のようになる。

【0059】P11： 担当者1は、文書をサーバ11に送って、文書の作成を通知する。

P12： サーバ11は、適当な値を一つ生成し、文書が回送される順に各担当者の関数を値に適用し、適用結果81を秘密情報として、IDとともに秘密情報記憶装置30に格納する。適用結果81は、図5の秘密情報と同様に、関数値“関数3（関数2（関数1（値）））”を表す。そして、関数を適用する前の値をIDとともに担当者1の端末12に送る。このとき、サーバ11は値を暗号化してから送ってもよい。

【0060】P13： 端末12は、送られてきた値に関数1を適用し、文書、ID、適用結果82、および電子署名1を、担当者2の端末13に送る。

P14： 端末13は、送られてきた値に関数2を適用し、文書、ID、適用結果83、電子署名1、および電子署名2を、担当者3の端末14に送る。

【0061】P15： 端末14は、送られてきた値に関数3を適用し、文書、ID、適用結果84、電子署名1、電子署名2、および電子署名3を、サーバ11に送る。サーバ11は、送られてきた値84と秘密情報記憶装置30に格納された秘密情報81を比較し、それらが同じであれば文書が正しく回送されたとみなす。

【0062】図9は、図8の認証システムにおける関数の適用結果（関数値）の具体例を示している。図9における処理は、次の通りである。

P21： 担当者1は、文書をサーバ11に送って、文書の作成を通知する。

【0063】P22： サーバ11は、ID“1”と、一つのランダムな値“i75x3fw0”を生成し、文書が回送される順に各担当者の関数を値に適用し、関数値“s9ih6rug”を得る。次に、この関数値を秘密情報として、ID“1”とともに秘密情報記憶装置30に格納する。そして、関数を適用する前の値“i75x3fw0”を、ID“1”とともに担当者1の端末12に送る。

【0064】P23： 端末12は、送られてきた値“i75x3fw0”に関数1を適用して、関数値“nnqo18j6”を得る。そして、文書、ID“1”、

および関数値“nnqo18j6”に電子署名1を付けて、担当者2の端末13に送る。

【0065】P24： 端末13は、電子署名1を検証した後、送られてきた値“nnqo18j6”に関数2を適用し、関数値“pge5b92h”を得る。そして、文書、ID“1”、および関数値“pge5b92h”に電子署名2を付けて、担当者3の端末14に送る。

【0066】P25： 端末14は、電子署名2を検証した後、送られてきた値“pge5b92h”に関数3を適用し、関数値“s9ih6rug”を得る。そして、文書、ID“1”、および関数値“s9ih6rug”に電子署名3を付けて、サーバ11に送る。サーバ11は、送られてきた値“s9ih6rug”と秘密情報記憶装置30に格納された秘密情報“s9ih6rug”を比較し、それらが同じであるので、文書が正しく回送されたとみなす。

【0067】図10は、関数として公開鍵暗号システムにおける復号化関数を用いた認証システムを示している。公開鍵暗号システムとは、RSA (Rivest-Shamir-Adleman) 暗号のような公開鍵暗号アルゴリズムを用いたシステムである。

【0068】公開鍵暗号システムにおいては、暗号化に秘密鍵を用い、復号化に公開鍵を用いており、一般に、誰でも復号化を行うことができる。しかし、ここでは、各担当者毎に異なる復号化鍵を用いた復号化関数を与えられ、それらの鍵情報を担当者は知らないものとする。復号化のアルゴリズムは、担当者毎に異なっても同じでもよい。図10において、担当者1が文書を作成する場合の処理は、次のようになる。

【0069】P31： 担当者1は、文書をサーバ11に送って、文書の作成を通知する。

P32： サーバ11は、適当な値91を一つ生成し、それを秘密情報として、IDとともに秘密情報記憶装置30に格納する。そして、文書が回送される順序とは逆の順序で各担当者の暗号関数を値に適用し、適用結果92をIDとともに担当者1の端末12に送る。適用結果92は、関数値“暗号関数1（暗号関数2（暗号関数3（値）））”を表す。

【0070】P33： 端末12は、送られてきた値に復号関数1を適用し、文書、ID、復号結果93、および電子署名1を、担当者2の端末13に送る。復号結果93は、関数値“暗号関数2（暗号関数3（値））”を表す。

【0071】P34： 端末13は、送られてきた値に復号関数2を適用し、文書、ID、復号結果94、電子署名1、および電子署名2を、担当者3の端末14に送る。復号結果93は、関数値“暗号関数3（値）”を表す。

【0072】P35： 端末14は、送られてきた値に

復号関数3を適用し、文書、ID、復号結果95、電子署名1、電子署名2、および電子署名3を、サーバ11に送る。サーバ11は、送られてきた値95と秘密情報記憶装置30に格納された秘密情報91を比較し、それらが同じであれば文書が正しく回送されたとみなす。

【0073】このように、担当者に与える関数に公開鍵暗号アルゴリズムを用い、その鍵情報を担当者に知らせないことで、鍵情報を含めた各担当者の関数を推定することが困難になり、システムの信頼性が向上する。

【0074】次に、図11から図17までを参照しながら、サーバ11と各端末の処理のフローを説明する。図11は、サーバ11による関数発生処理のフローチャートである。処理が開始されると、関数発生部25は、担当者毎に個別の関数を発生させる(ステップS1)。次に、サーバ11は、各関数を関数記憶装置29に格納した後(ステップS2)、各担当者に配送し(ステップS3)、処理を終了する。

【0075】図12は、端末による関数格納処理のフローチャートである。処理が開始されると、端末は、サーバ11が発生させた関数を受け取り(ステップS11)、それを端末の関数記憶装置に格納して(ステップS12)、処理を終了する。

【0076】図13は、端末による文書発信依頼処理のフローチャートである。処理が開始されると、端末は、担当者からの指示に従って文書を作成し(ステップS21)、それをサーバ11に送って(ステップS22)、処理を終了する。

【0077】図14は、文書発信依頼を受けたサーバ11による値発生処理のフローチャートである。処理が開始されると、サーバ11は、端末から文書を受け取り(ステップS31)、値発生部26は、IDと適当な値を発生させる(ステップS32)。

【0078】次に、関数適用部27は、文書の種別と発信者の情報をもとに、図3に示したような関数記憶装置29のデータから、文書の回送ルートを検索する(ステップS33)。そして、値発生部26が発生した値に、各担当者の関数を回送ルートの順に適用し(ステップS34)、適用結果とIDを秘密情報記憶装置30に格納する(ステップS35)。サーバ11は、IDと関数適用前の値を文書発信を依頼してきた担当者の端末に送り(ステップS36)、処理を終了する。

【0079】図15は、文書発信を依頼した担当者の端末による文書回送処理のフローチャートである。処理が開始されると、端末は、サーバ11からIDと値を受け取る(ステップS41)。次に、関数適用部は、端末に付属する関数記憶装置から関数を取り出し(ステップS42)、それを受け取った値に適用する(ステップS43)。

【0080】そして、署名作成部は、文書とIDと関数値に電子署名を付けて(ステップS44)、それらを次

の担当者の端末に送り(ステップS45)、処理を終了する。

【0081】図16は、文書の回送を受けた担当者の端末による文書回送処理のフローチャートである。処理が開始されると、端末は、他の担当者の端末から、その担当者の電子署名付きの文書とIDと関数値を受け取る(ステップS51)。次に、署名検証部は、その電子署名を検証して(ステップS52)、それが正しいかどうかを判定する(ステップS53)。

【0082】検証結果が正しいければ、次に、関数適用部は、端末に付属する関数記憶装置から関数を取り出し(ステップS54)、それを受け取った関数値に適用する(ステップS55)。

【0083】そして、署名作成部は、文書とIDと新しい関数値に電子署名を付けて(ステップS56)、それらを次の担当者の端末またはサーバ11に送り(ステップS57)、処理を終了する。

【0084】ステップS53において検証結果が正しくなければ、文書回送処理を中断し(ステップS58)、エラー処理を行って、処理を終了する。エラー処理では、例えば、電子署名が正しくないことがサーバ11に通知され、それがサーバ11から対応する担当者に通知される。

【0085】図17は、最後の担当者から文書の回送を受けたサーバ11による文書発信処理のフローチャートである。処理が開始されると、サーバ11は、その担当者の電子署名付きの文書とIDと関数値を受け取る(ステップS61)。次に、署名検証部24は、その電子署名を検証して(ステップS62)、それが正しいかどうかを判定する(ステップS63)。検証結果が正しいければ、次に、秘密情報比較部28は、秘密情報記憶装置30から登録されている関数値を取り出し(ステップS64)、それを受け取った関数値と比較して(ステップS65)、それらが同じかどうかを判定する(ステップS66)。そして、それらが同じであれば、受け取った文書を文書記憶装置31に格納する(ステップS67)。

【0086】次に、文書発信部22は、その文書に代表の電子署名を付けて、社外に発信し(ステップS68)、処理を終了する。ステップS63において検証結果が正しくないとき、および、ステップS66において2つの値が同じでないときは、文書発信処理を中断し(ステップS69)、エラー処理を行って、処理を終了する。

【0087】ステップS63において検証結果が正しくなければ、エラー処理では、例えば、電子署名が正しくないことが対応する担当者に通知される。また、ステップS66において2つの値が同じでなければ、エラー処理では、例えば、回送が正しく行われなかったことが文書の作成者および関連する担当者に通知される。

【0088】以上説明した実施形態において、一般に、

関数は役職に対して一意的に設定され、担当者が変わっても変化しない。しかし、担当者が変わる度に関数を取り替えることで、より安全性の高いシステムを実現することもできる。

【0089】また、本発明の認証システムは、文書だけでなく、画像、音声、プログラムなどの任意の電子情報の回送および発信を認証する技術に適用可能であり、本発明の認証方法は、紙媒体などを含む任意の情報の回送および発信を認証する技術に適用可能である。

【0090】

【発明の効果】本発明によれば、企業間で電子取引が行われる場合に、まず、企業内で電子情報が正しく回送されたことを検証することで、各担当者に権限があるかどうかを確認することができる。そして、正しく回送された場合にのみ、企業の代表の電子署名を付けることで、電子情報を発信する企業における不正取引を防止することができる。

【0091】本発明は、電子取引において不正取引を防止するための一つの技術を提供しており、今後、電子取引を開始しようとする企業において、その利用が期待される。

【図面の簡単な説明】

【図1】本発明の認証システムの原理図である。

【図2】認証システムの構成図である。

【図3】関数記憶装置のデータを示している。

【図4】第1の通信データを示している。

【図5】秘密情報記憶装置のデータを示している。

【図6】第2の通信データを示している。

【図7】情報処理装置の構成図である。

【図8】第1の実施形態を示す図である。

【図9】関数値の例を示す図である。

【図10】第2の実施形態を示す図である。

【図11】関数発生処理のフローチャートである。

【図12】関数格納処理のフローチャートである。

【図13】文書発信依頼処理のフローチャートである。

【図14】値発生処理のフローチャートである。

【図15】第1の文書回送処理のフローチャートである。

る。

【図16】第2の文書回送処理のフローチャートである。

【図17】文書発信処理のフローチャートである。

【符号の説明】

- 1 認証装置
- 2 秘密情報格納手段
- 3 確認手段
- 4 端末装置
- 5 通信手段
- 6 変換手段
- 7 通信ネットワーク
- 11 サーバ
- 12、13、14 端末
- 21、41、51、61 インタフェース
- 22 文書発信部
- 23、44、54、64 署名作成部
- 24、42、52、62 署名検証部
- 25 関数発生部
- 26 値発生部
- 27 関数適用部
- 28 秘密情報比較部
- 29、45、55、65 関数記憶装置
- 30 秘密情報記憶装置
- 31 文書記憶装置
- 71 CPU
- 72 メモリ
- 73 入力装置
- 74 出力装置
- 75 外部記憶装置
- 76 媒体駆動装置
- 77 ネットワーク接続装置
- 78 バス
- 79 可搬記録媒体
- 80 他の情報処理装置
- 81、82、83、84、92、93、94 関数値
- 91、95 値

【図3】

関数記憶装置のデータを示す図

文書種別	発信者	受信者	関数
文1	担当者1	担当者2	関数1
文1	担当者2	担当者3	関数2
文1	担当者3	サーバ	関数3

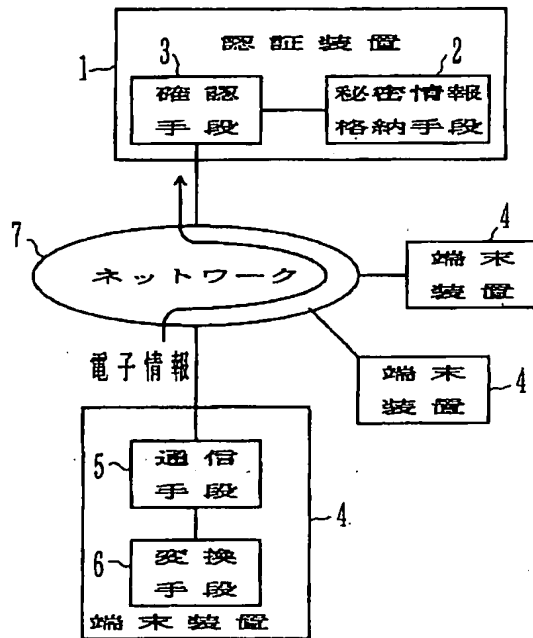
【図5】

秘密情報記憶装置のデータを示す図

ID	秘密情報
1	関数3 (関数2 (関数1 (値)))

【図1】

本発明の原理部



【図4】

第1の通信データを示す図

手続	通信データ	
	文書	値
P1	ID	
P2	ID	電子署名1
P3	ID	関数1 (値)
P4	ID	関数2 (関数1 (値))
P5	ID	関数3 (関数2 (関数1 (値)))

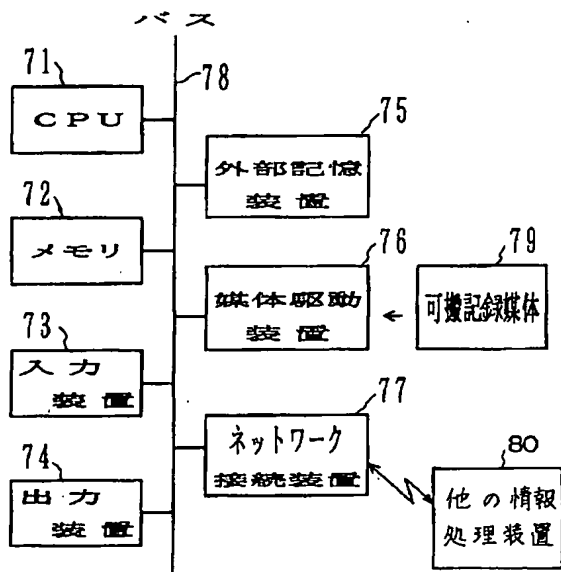
【図6】

第2の通信データを示す図

手続	通信データ	
	文書	値
P1	ID	電子署名0
P2	ID	関数1 (値)
P3	ID	電子署名0, 電子署名1
P4	ID	関数2 (関数1 (値))
P5	ID	関数3 (関数2 (関数1 (値)))

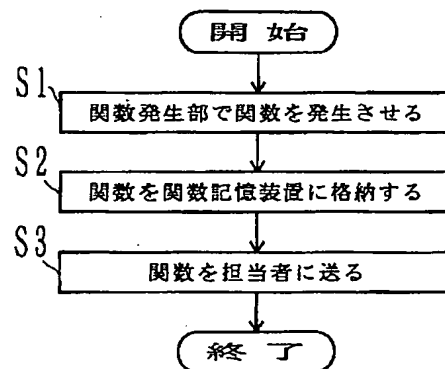
【図7】

情報処理装置の構成図



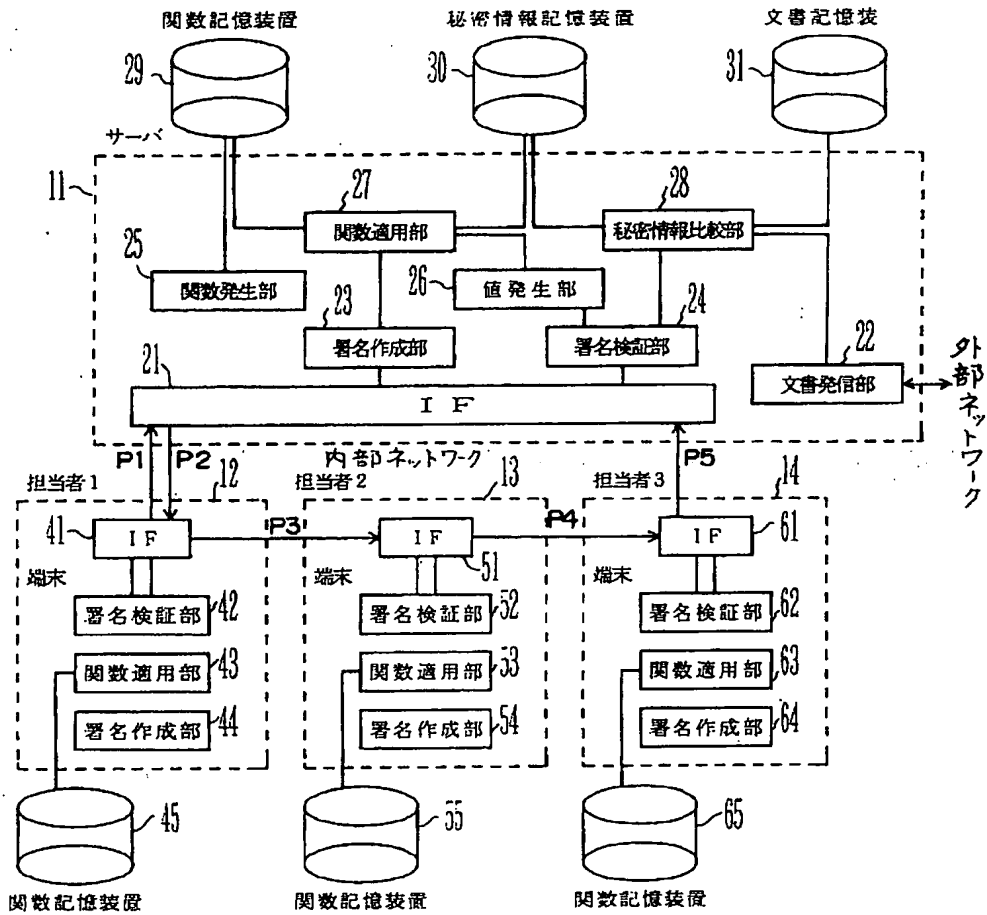
【図11】

関数発生処理のフローチャート



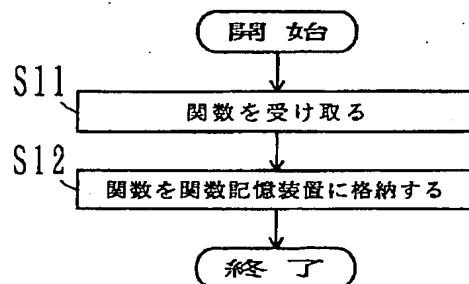
【図2】

認証システムの構成図



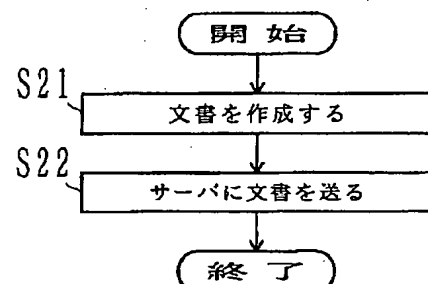
【図12】

関数格納処理のフローチャート



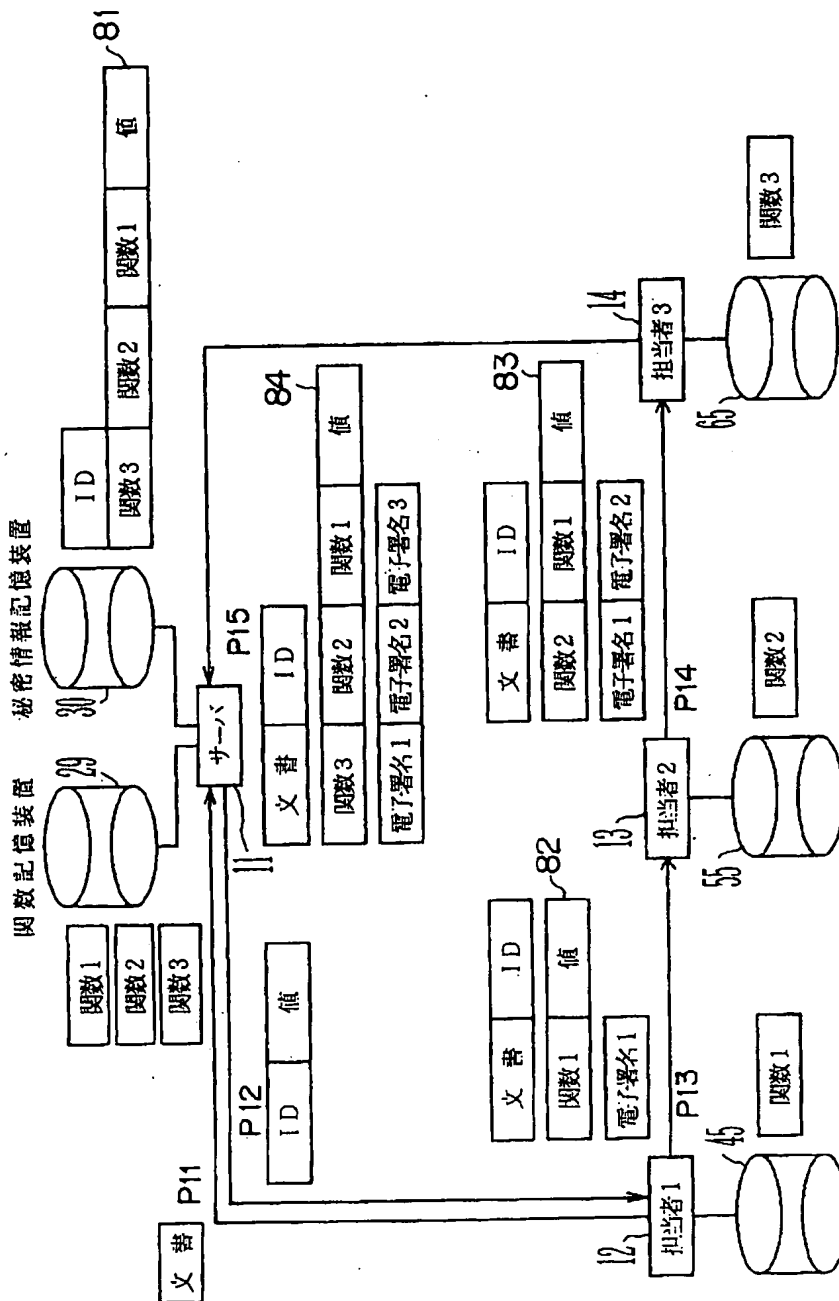
【図13】

文書発信依頼処理のフローチャート



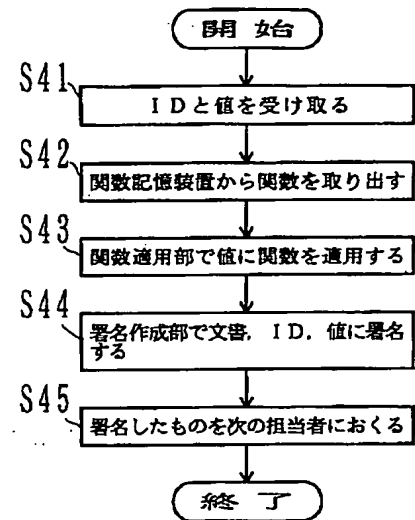
【図8】

第1の実施形態を示す図



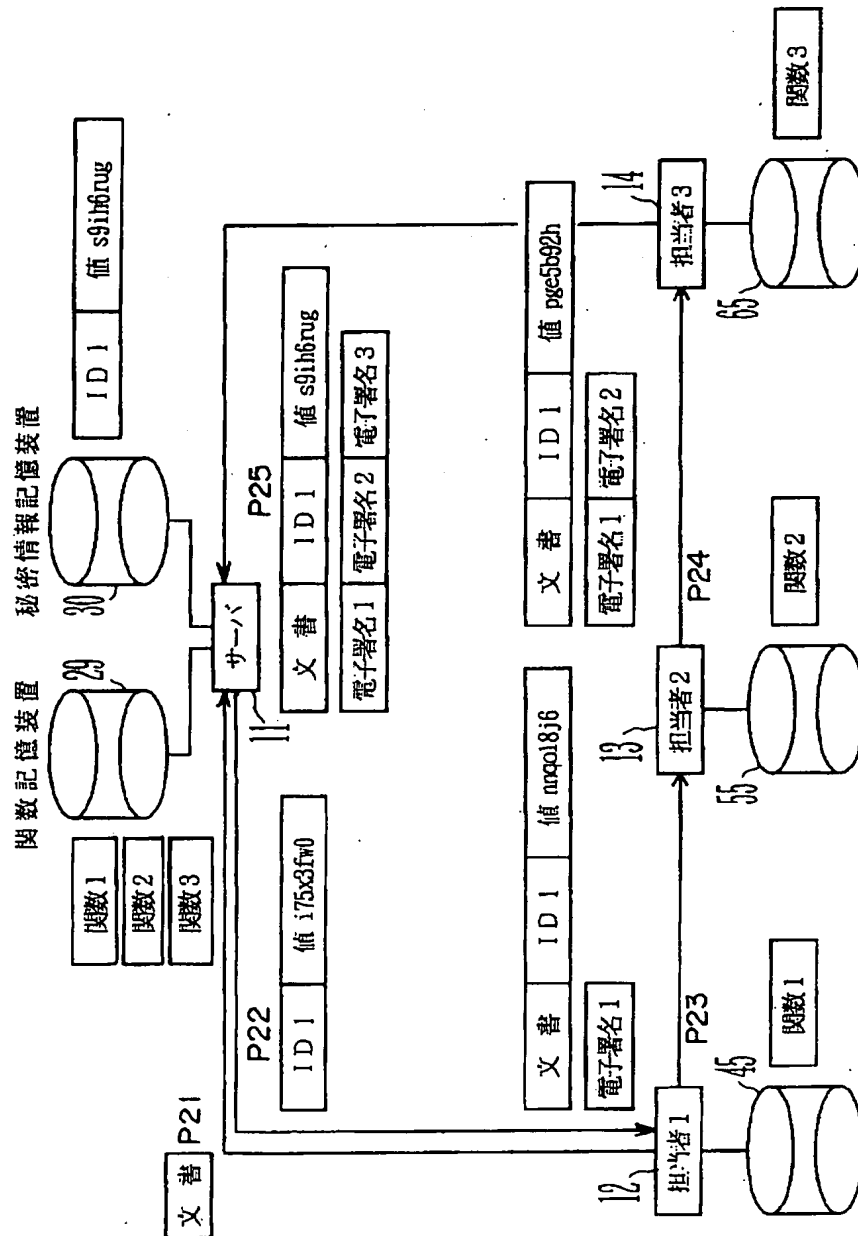
【図15】

第1の文書回送処理のフローチャート



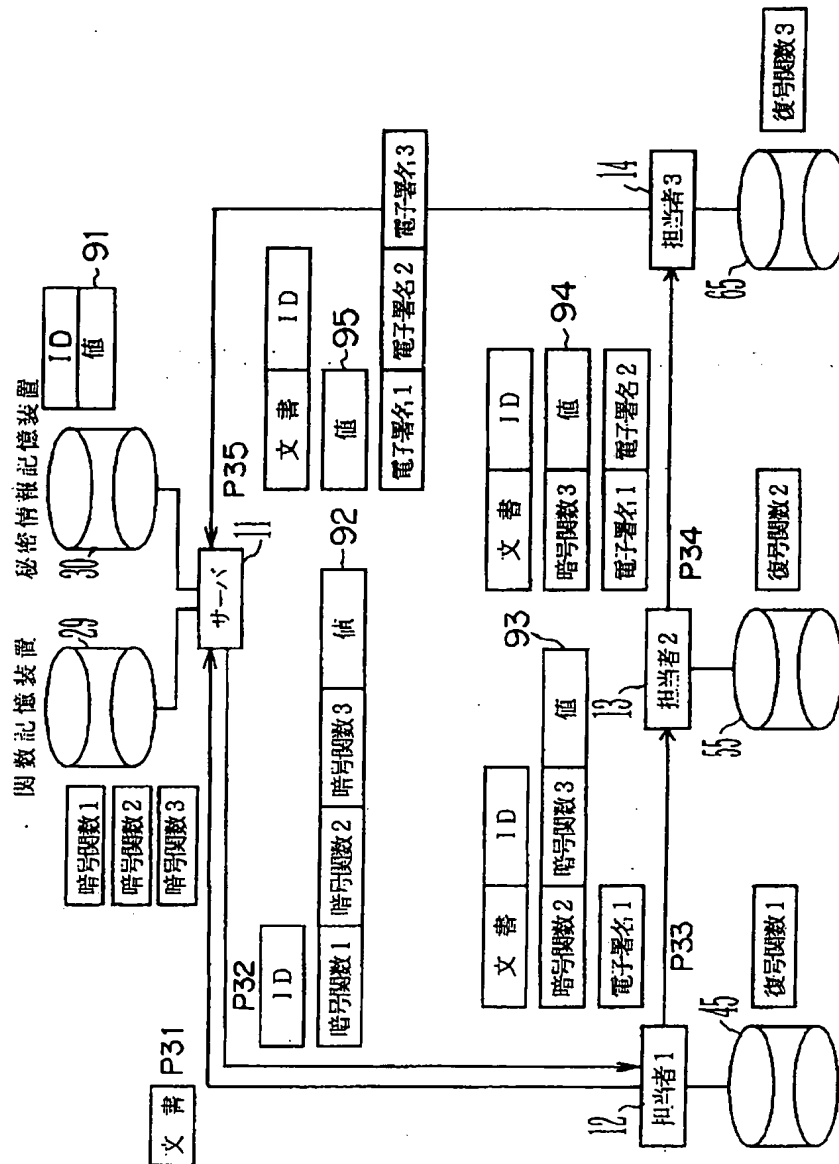
【図9】

関数値の例を示す図



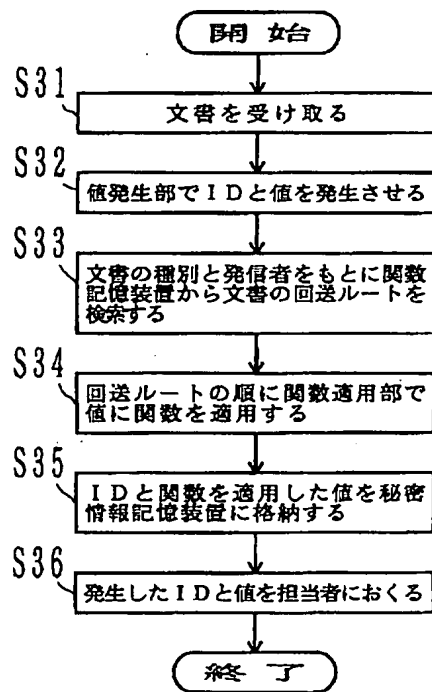
【図10】

第2の実施形態を示す図



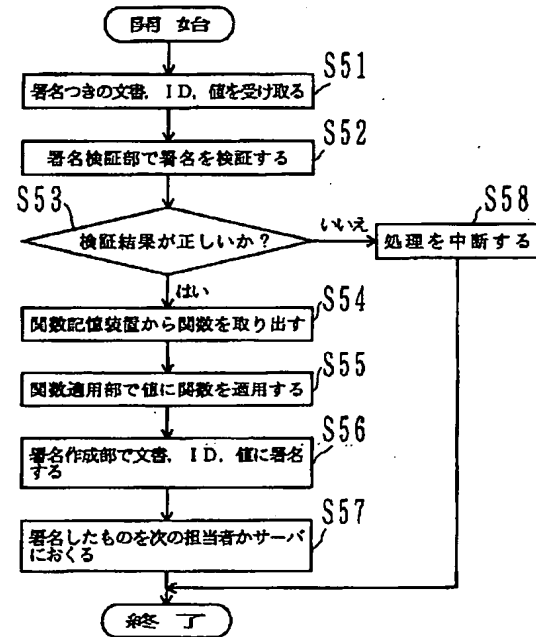
【図14】

値発生処理のフローチャート



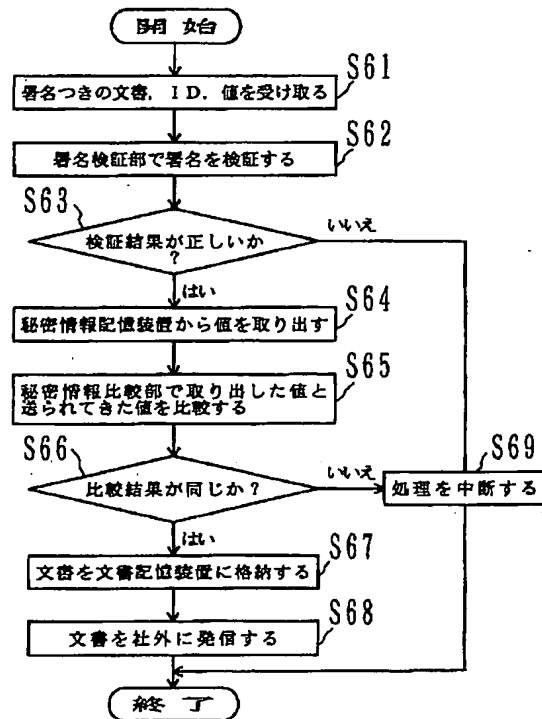
【図16】

第2の文書回送処理のフローチャート



【図17】

文書発信処理のフローチャート



フロントページの続き

(51) Int. Cl. 6

識別記号

FI

H04L 9/00

675A

(72) 発明者 黒田 康嗣

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(72) 発明者 鳥居 悟

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内